(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平８－３３５０４０

(43)公開日　平成８年（１９９６）１２月１７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
G09C 1/00		7259-5J	G09C 1/00		
H04H 1/00			H04H 1/00	F	
1/02			1/02	E	
H04L 9/00			H04L 9/00	Z	
9/10			H04N 7/167		

審査請求　未請求　請求項の数５　ＦＤ　（全１２頁）　最終頁に続く

(21)出願番号　特願平７－１５９７７１

(22)出願日　平成７年（１９９５）６月２日

(71)出願人　０００００５２２３
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中１０１５番地　富士通株式会社内

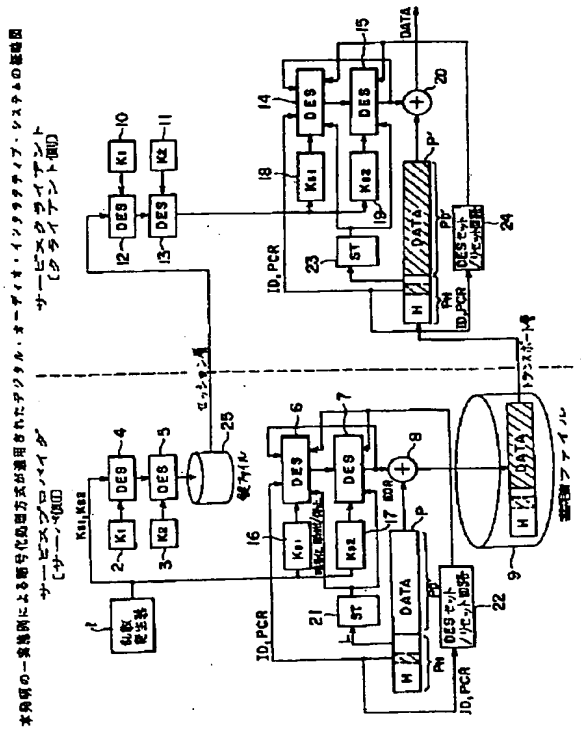
(72)発明者　宗像　昭夫
神奈川県川崎市中原区上小田中１０１５番地　富士通株式会社内

(74)代理人　弁理士　遠山　勉　（外１名）

最終頁に続く

(54)【発明の名称】暗号化処理方式

(57)【要約】
【目的】暗号化アルゴリズムを強化することによって鍵の頻繁な変更を減らし、サービスプロバイダーサービスクライアント間の情報転送効率を向上させることができる暗号化処理方式を提供する。
【構成】乱数発生器１は、乱数に基づき第１タイトル鍵Ｋｓ１及び第２タイトル鍵Ｋｓ２を生成する。タイトル用第１ＤＥＳ暗号化回路６は、入力情報を第１タイトル鍵Ｋｓ１によって暗号化する。この入力情報の初期値は、パケットのヘッダから抽出されたデータ識別ＩＤ及び相対時刻情報（ＰＣＲ）である。初期値の暗号化を完了した後では、タイトル用第２ＤＥＳ暗号化回路７の暗号化結果が入力情報となる。このタイトル用第２ＤＥＳ暗号化回路７は、タイトル用第１ＤＥＳ暗号化回路６による暗号化結果値を第２タイトル鍵Ｋｓ２によって暗号化する。排他ＯＲ回路８は、パケットに格納されたデータとタイトル用第２ＤＥＳ暗号化回路７の暗号化結果値との排他論理和を出力する。これが暗号化データとなる。



1

【特許請求の範囲】

【請求項１】データを提供するサービスプロバイダとデータの供給を受けるサービスクライアントとの間で配送される前記データを暗号化する暗号化処理方式において、

前記サービスプロバイダは、

乱数に基づき２つの鍵を生成する鍵生成手段と、

この鍵生成手段により生成された２つの鍵によりデータを暗号化する第１の暗号化手段と、

この第１の暗号化手段によって暗号化された前記データを前記サービスクライアントに配送するデータ配送手段と、

前記２つの鍵を特定内容のマスタ鍵によって暗号化する第２の暗号化手段と、

この第２の暗号化手段によって暗号化された前記２つの鍵を前記サービスクライアントに配送する鍵配送手段とを備え、

前記サービスクライアントは、

前記鍵配送手段によって配送された前記暗号化された２つの鍵を前記特定内容のマスタ鍵によって復号化する第１の復号化手段と、

この第１の復号化手段によって復号化された前記２つの鍵により前記データ配送手段によって配送された前記暗号化されたデータを復号化する第２の復号化手段とを備えたことを特徴とする暗号化処理装置。

【請求項２】パケットに格納されたデータをサービスクライアントに配送するサービスプロバイダにおける暗号化処理方式において、

乱数に基づき第１の鍵及び第２の鍵を生成する鍵生成手段と、

入力情報を前記第１の鍵によって暗号化する第１の暗号化回路と、

前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第１の暗号化回路に前記入力情報の初期値として入力する抽出手段と、

前記第１の暗号化回路による暗号化結果値を前記第２の鍵によって暗号化するとともに、この暗号化結果値を前記第１の暗号化回路に前記入力情報として更新入力する第２の暗号化回路と、

前記パケットに格納されたデータと前記第２の暗号化回路の暗号化結果値との排他論理和を出力する排他ＯＲ回路とを備えたことを特徴とする暗号化処理方式。

【請求項３】前記パケットは、このパケットに格納されているデータの格納位置についての格納位置情報を含んでいるとともに、

この格納位置情報に基づいて、前記データが前記排他ＯＲ回路に入力されている時点でのみ前記第１の暗号化回路及び前記第２の暗号化回路による暗号化を可能とする暗号化制御回路とを更に備えたことを特徴とする請求項２記載の暗号化処理装置。

2

【請求項４】前記パケットから前記時刻情報を検出して、前記第１の暗号化回路及び前記第２の暗号化回路の状態を初期化する初期化手段を更に備えたことを特徴とする請求項２記載の暗号化処理装置。

【請求項５】データを提供するサービスプロバイダとデータの供給を受けるサービスクライアントとの間でパケットに格納されて配送される前記データを暗号化する暗号化処理方式において、

前記サービスプロバイダは、

乱数に基づき第１の鍵及び第２の鍵を生成する鍵生成手段と、

この第１の鍵及び第２の鍵を前記サービスクライアントに配送する鍵配送手段と、

入力情報を前記第１の鍵によって暗号化する第１の暗号化回路と、

前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第１の暗号化回路に前記入力情報の初期値として入力する第１の抽出手段と、

前記第１の暗号化回路による暗号化結果値を前記第２の鍵によって暗号化するとともに、この暗号化結果値を前記第１の暗号化回路に前記入力情報として更新入力する第２の暗号化回路と、

前記パケットに格納されたデータと前記第２の暗号化回路の暗号化結果値との排他論理和を出力する第１の排他ＯＲ回路と、

この排他ＯＲ回路から出力されデータを格納した前記パケットを前記サービスクライアントに配送するデータ配送手段とを備え、

前記サービスクライアントは、

入力情報を前記第１の前記鍵配送手段によって配送された前記第３の鍵によって暗号化する第３の暗号化回路と、

前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第１の暗号化回路に前記入力情報の初期値として入力する第２の抽出手段と、

前記第３の暗号化回路による暗号化結果値を前記第２の鍵によって暗号化するとともに、この暗号化結果値を前記第３の暗号化回路に前記入力情報として更新入力する第４の暗号化回路と、

前記パケットに格納されたデータと前記第４の暗号化回路の暗号化結果値との排他論理和を出力する第２の排他ＯＲ回路とを備えたことを特徴とする暗号化処理方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、クライアントからの要求に応じて、映像著作物等のソフトウエアを通信手段を介して配送するシステム（デジタル・オーディオ・インタラクティブ・システム）において、特定の鍵によってこのソフトウェアを暗号化するための暗号化処理方式に関する。

【０００２】

【従来の技術】近年、ケーブルテレビジョンシステムや通信衛星を用いた通信システムの構築を背景に、デジタル情報化されたソフトウェア（音声データ，映像データ等，以下、「データ」という）を各家庭等に配送するサービスが提案されている。このサービスシステムは、ビデオ・オン・デマンド方式等と呼ばれるデジタル・オーディオ・インタラクティブ・システムである。このデジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者とユーザとの間で電話線等を介した通信が行われる。そして、サービス提供者は、ユーザから要求された時刻に要求された内容のデータをこのユーザに配送するとともに、このデータの使用料金をクレジットカード会社等を通じて当該ユーザに課金し、その一部をコンテンツ供給者に還元するのである。

【０００３】このようなデジタル・オーディオ・インタラクティブ・システムが普及してゆく上で重要な事は、インフラストラクチャーとなるサーバ/ ネットワーク/ ターミナルが低コストで構築されることは勿論であるが、これらを媒介としてユーザに提供されるデータが豊富に準備されなければ、成功とはならないということである。即ち、データとインフラストラクチャは車の両輪であるので、データ提供者がコンテンツ提供による利益回収を見込めるとともに不測の損害を被る危険がない仕組みをこのインフラストラクチャに組み込むことにより、データが集まりやすい環境を整備することが不可欠なのである。なお、このような仕組みは、データ提供者とユーザとを媒介する供給メディアの種類（広帯域ケーブルネットワーク，衛星システム，移動通信，光メディアパッケージ等）に拘わらず、整備されていなければならない。

【０００４】従って、配送中においてデータが無権利の第三者（当該データの使用料を支払っていない第三者）に傍受されて不当に使用（再生）されることがないよう、配送中においてデータは暗号化されていた。従来における暗号化処理方式を、図６によって説明する。

【０００５】図６において、サービスプロバイダ（サービス提供者側システムのことをいう。以下同じ）の第１暗号化回路１０３は、パケットフォーマットのデータを一個の鍵（Ｋｓ）のみで暗号化し、トランスポート層伝送路を通じてサービスクライアント（ユーザ側システムのことをいう。以下同じ）に配送する。この暗号化されたデータを受け取ったサービスクライアントの第１復号化回路１０６は、第１暗号化回路１０３にて暗号化に用いられた鍵（Ｋｓ）により、データを復号化する。このように従来の暗号化処理方式ではデータの暗号化及び復号化のアルゴリズムは一個の鍵（Ｋｓ）を用いた一段階のみの脆弱なものであったので、鍵（Ｋｓ）の解読を防ぐため、鍵（Ｋｓ）を頻繁に変更する必要があった。また、通信路の誤り及び切断から速やかに復旧する為、暗

号同期信号を送信することが必要であった。

【０００６】この条件を満足するため、図６に示すように、サービスプロバイダに乱数発生器１００，マスタ鍵（Ｋ１）１０１及び第２暗号化回路１０２を設け、サービスクライアントに、マスタ鍵（Ｋ１）１０４及び第２復号化回路１０２を設けている。

【０００７】この乱数発生器１００は、常時継続的に乱数系列を発生している。そして、この乱数系列が数秒間隔で鍵ブロック単位（予め定められた鍵の桁）で切り出され、数秒間隔で更新される鍵（Ｋｓ）として第１暗号化回路１０３に入力される。このように更新される鍵（Ｋｓ）はサービスクライアントにも配送されなければならないので、第２の暗号化回路１０２は、乱数発生器１００から切り出される鍵（Ｋｓ）をマスタ鍵（Ｋ１）１０１で暗号化し、トランスポート層のユーザ割当パケットの一部（セッション層）を利用してサービスクライアントに配送する。サービスクライアントの第２復号化回路１０５は、暗号化された鍵（Ｋｓ）をマスタ鍵（Ｋ１）を用いて復号化し、第１復号化回路１０６に入力していた。

【０００８】そして、第１暗号化回路１０３及び第１復号化回路１０６は、新たな鍵（Ｋｓ）の入力がある毎に自らをリセットして同期を取り、それ以降のデータを新たな鍵（Ｋｓ）によって暗号化・復号化する。なお、マスタ鍵（Ｋ１）１０１，１０４は、サービスプロバイダ及びサービスクライアントに、夫々予め同内容で用意された固定鍵である。

【０００９】このようにして、従来のデータ暗号化処理方式では、鍵（Ｋｓ）の変更及び暗号同期処理を行っていた。

【００１０】

【発明が解決しようとする課題】しかしながら、上記従来の暗号化処理方式にあっては、数秒間隔で、新たな鍵（Ｋｓ）をサービスプロバイダからサービスクライアントに配送しなければならないので、本来のデータ配送に使用するパケット以外に、大量のパケット（鍵配送用パケット）を転送しなければならなかった。その結果、サービスプロバイダーサービスクライアント間の情報転送効率が著しく低下してしまっていた。

【００１１】本発明の第１の課題は、暗号化アルゴリズムを強化することによって鍵の頻繁な変更の必要を減らし、サービスプロバイダーサービスクライアント間の情報転送効率を向上させることができる暗号化処理方式を提供することである。

【００１２】また、本発明の第２の課題は、データの転送に用いるパケットヘッダ上の相対時刻情報を暗号化の初期値に利用して、同じ内容のデータを発生時刻に依り別内容の暗号化データとし、解読を困難にすることができる暗号化処理方式を提供することである。

【００１３】

5

【課題を解決するための手段】

（第１の態様）本発明の第１の態様は、専ら上記第１の課題を、サービスプロバイダーサービスクライアント間で解決するためになされたものである。即ち、図１の原理図に示したように、データを提供するサービスプロバイダとデータの供給を受けるサービスクライアントとの間で配送される前記データを暗号化する暗号化処理方式において、前記サービスプロバイダは、乱数に基づき２つの鍵（Ｋｓ１，Ｋｓ２）を生成する鍵生成手段（乱数発生器１１０）と、この鍵生成手段（乱数発生器１１０）により生成された２つの鍵（Ｋｓ１，Ｋｓ２）によりデータを暗号化する第１の暗号化手段（１１３）と、この第１の暗号化手段（１１３）によって暗号化された前記データを前記サービスクライアントに配送するデータ配送手段（トランスポート層伝送路）と、前記２つの鍵（Ｋｓ１，Ｋｓ２）を特定内容のマスタ鍵（Ｋ１，１０１）によって暗号化する第２の暗号化手段（１１２）と、この第２の暗号化手段（１１２）によって暗号化された前記２つの鍵（Ｋｓ１，Ｋｓ２）を前記サービスクライアントに配送する鍵配送手段（セッション層伝送路）とを備え、前記サービスクライアントは、前記鍵配送手段（セッション層伝送路）によって配送された前記暗号化された２つの鍵（Ｋｓ１，Ｋｓ２）を前記特定内容のマスタ鍵（Ｋ１，１１４）によって復号化する第１の復号化手段（１１５）と、この第１の復号化手段（１１５）によって復号化された前記２つの鍵（Ｋｓ１，Ｋｓ２）により前記データ配送手段（トランスポート層伝送路）によって配送された前記暗号化されたデータを復号化する第２の復号化手段（１１６）とを備えたことを特徴とする（請求項１に対応）。

（第２の態様）本発明の第２の態様は、上記第１及び第２の課題を、サービスプロバイダ側で解決するためになされたものである。即ち、パケットに格納されたデータをサービスクライアントに配送するサービスプロバイダにおける暗号化処理方式において、乱数に基づき第１の鍵及び第２の鍵を生成する鍵生成手段と、入力情報を前記第１の鍵によって暗号化する第１の暗号化回路と、前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第１の暗号化回路に前記入力情報の初期値として入力する抽出手段と、前記第１の暗号化回路による暗号化結果値を前記第２の鍵によって暗号化するとともに、この暗号化結果値を前記第１の暗号化回路に前記入力情報として更新入力する第２の暗号化回路と、前記パケットに格納されたデータと前記第２の暗号化回路の暗号化結果値との排他論理和を出力する排他ＯＲ回路とを備えたことを特徴とする（請求項２に対応）。

（第３の態様）本発明の第３の態様は、上記第１及び第２の課題を、サービスプロバイダーサービスクライアント間で解決するためになされたものである。即ち、データを提供するサービスプロバイダとデータの供給を受けるサービスクライアントとの間でパケットに格納されて配送される前記データを暗号化する暗号化処理方式において、前記サービスプロバイダは、乱数に基づき第１の鍵及び第２の鍵を生成する鍵生成手段と、この第１の鍵及び第２の鍵を前記サービスクライアントに配送する鍵配送手段と、入力情報を前記第１の鍵によって暗号化する第１の暗号化回路と、前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第１の暗号化回路に前記入力情報の初期値として入力する第１の抽出手段と、前記第１の暗号化回路による暗号化結果値を前記第２の鍵によって暗号化するとともに、この暗号化結果値を前記第１の暗号化回路に前記入力情報として更新入力する第２の暗号化回路と、前記パケットに格納されたデータと前記第２の暗号化回路の暗号化結果値との排他論理和を出力する第１の排他ＯＲ回路と、この排他ＯＲ回路から出力されデータを格納した前記パケットを前記サービスクライアントに配送するデータ配送手段とを備え、前記サービスクライアントは、入力情報を前記第１の前記鍵配送手段によって配送された前記第１の鍵によって暗号化する第３の暗号化回路と、前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第３の暗号化回路に前記入力情報の初期値として入力する第２の抽出手段と、前記第３の暗号化回路による暗号化結果値を前記第２の鍵によって暗号化するとともに、この暗号化結果値を前記第３の暗号化回路に前記入力情報として更新入力する第４の暗号化回路と、前記パケットに格納されたデータと前記第４の暗号化回路の暗号化結果値との排他論理和を出力する第２の排他ＯＲ回路とを備えたことを特徴とする（請求項５に対応）。

【００１４】

【作用】

（請求項１の作用）サービスプロバイダ内において鍵生成手段は、乱数に基づき２つの鍵を生成する。第１の暗号化手段は、この鍵生成手段により生成された２つの鍵に基づいて所定の暗号化アルゴリズムを実行することにより、データを暗号化する。また、第２の暗号化手段は、この２つの鍵を特定内容のマスタ鍵によって暗号化する。以上の後、データ配送手段は、第１の暗号化手段によって暗号化されたデータをサービスクライアントに配送し、鍵配送手段は、第２の暗号化手段によって暗号化された２つの鍵をサービスクライアントに配送する。

【００１５】一方、サービスクライアント内において、第１の復号化手段は、鍵配送手段によって配送された暗号化された２つの鍵を特定内容のマスタ鍵によって復号化する。第２の復号化手段は、この第１の復号化手段によって復号化された２つの鍵に基づいて、上記暗号化アルゴリズムに対応する復号化アルゴリズムを実行することにより、データ配送手段によって配送された暗号化されたデータを復号化する。

【００１６】このように、２つの鍵によって暗号化を行

っているので暗号化強度が強くなる。

（請求項２の作用）鍵生成手段は、乱数に基づき第１の鍵及び第２の鍵を生成する。第１の暗号化回路は、入力情報を第１の鍵によって暗号化する。この入力情報の初期値は、抽出手段によってパケットのヘッダから抽出された時刻情報である。初期値の暗号化を完了した後では、第２の暗号化回路の暗号化結果が入力情報となる。

【００１７】この第２の暗号化回路は、第１の暗号化回路による暗号化結果値を第２の鍵によって暗号化する。排他ＯＲ回路は、パケットに格納されたデータと第２の暗号化回路の暗号化結果値との排他論理和を出力する。

【００１８】このように、この暗号化処理方式では、暗号化のために第１の鍵，第２の鍵，及び時刻情報を用いている。そのため、暗号化強度がそれだけ向上する。しかも、時刻情報を用いているから、たとえ第１の鍵及び第２の鍵を暫く一定にしていたとしても、同じ内容のデータを別個の内容を持った暗号化データとすることができるので、それだけ第三者による解読が困難になる。

（請求項３の作用）パケットがこのパケットに格納されているデータの格納位置についての格納位置情報を含むようにし、暗号化制御回路がこの格納位置情報に基づいてデータが排他ＯＲ回路に入力されている時点でのみ第１の暗号化回路及び第２の暗号化回路による暗号化を可能とするように制御を行えば、パケットのデータ格納部分以外を平文のままとしておくことができるので、サービスクライアントは、この平文部分から時刻情報を読み出して復号を行うことができる。

（請求項４の作用）パケットから時刻情報を検出して第１の暗号化回路及び第２の暗号化回路の状態を初期化する初期化手段を更に備えれば、サービスクライアント側に特別な同期信号を送信しなくても、サービスクライアントは、この時刻情報を検出して自律的に暗号同期をとることができる。

（請求項５の作用）サービスプロバイダにおいて鍵生成手段は、乱数に基づき第１の鍵及び第２の鍵を生成する。鍵配送手段は、この第１の鍵及び第２の鍵をサービスクライアントに配送する。また、第１の暗号化回路は、入力情報を第１の鍵によって暗号化する。この入力情報の初期値は、第１抽出手段によってパケットのヘッダから抽出された時刻情報である。初期値の暗号化が完了した後では、第２の暗号化回路による暗号化結果が入力情報となる。この第２の暗号化回路は、第１の暗号化回路による暗号化結果値を第２の鍵によって暗号化する。第１の排他ＯＲ回路は、パケットに格納されたデータと第２の暗号化回路の暗号化結果値との排他論理和を出力する。データ配送手段は、このようにして暗号化されたデータを格納したパケットをサービスクライアントに配送する。

【００１９】一方、サービスクライアントにおいて第３の暗号化回路は、入力情報を第１の鍵鍵配送手段によって配送された第１の鍵によって暗号化する。この入力情報の初期値は、第２の抽出手段によってパケットのヘッダから抽出された時刻情報である。この初期値の暗号化が完了した後は、第４の暗号化回路による暗号化結果が入力情報となる。この第４の暗号化回路は、第３の暗号化回路による暗号化結果値を第２の鍵によって暗号化する。第２の排他ＯＲ回路は、パケットに格納されたデータと第４の暗号化回路の暗号化結果値との排他論理和を出力する。

【００２０】このように、この暗号化処理方式では、暗号化のために第１の鍵，第２の鍵，及び時刻情報を用いている。そのため、暗号化強度がそれだけ向上する。しかも、時刻情報を用いているから、たとえ第１の鍵及び第２の鍵を暫く一定にしていたとしても、同じ内容のデータを別個の内容を持った暗号化データとすることができるので、それだけ第三者による解読が困難になる。

【００２１】

【実施例】以下、図面に基づいて、本発明の一実施例の説明を行う。本実施例は、本発明による暗号化処理方式を、デジタル・オーディオ・インタラクティブ・システムに適用したものである。

《実施例の構成》

（ソフトウェの構成）先ず、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいて流通されるソフトウェアの構成を、図３に示す。図３に示されるように、一本のソフトウェアは、複数に分割されて、夫々別のトランスポートパケットＰに格納される。このトランスポートパケットＰは、ＭＰＥＧで規定されたものである。

【００２２】各トランスポートパケットＰの先頭には、夫々のトランスポートパケットＰに格納されているデータの状態を示すメインヘッダが付加されている。このメインヘッダには、データ識別ＩＤ（ＩＤ），相対時刻情報（ＰＣＲ），データ長情報（Ｌ），等の各種情報が含まれている。即ち、データ識別ＩＤは、或るソフトウェアを構成するデータを格納していることを示す識別子であり、同じソフトウェアを構成するデータを格納している全てのトランスポートパケットＰには同じデータ識別ＩＤが付されている。また、相対時刻情報（ＰＣＲ）は、各トランスポートパケットＰの生成時刻を示す情報であり、次々と送られたデータの順番に従ってアップデートされてソフトウェア全体が送り終えた段階で停止するものである。従って、この相対時刻情報（ＰＣＲ）の順番に、データ識別ＩＤを同じくする各トランスポートパケットＰに格納されているデータを並べることにより、元のソフトウェアを再構築することができる。また、格納位置情報としてのデータ長情報（Ｌ）は、このメインヘッダの後に続くデータの長さを示す情報である。

【００２３】各トランスポートパケットＰには、メイン

9

ヘッダに続いて、データとサブヘッダが交互に繋がっている。各データは、ＭＰＥＧ規格によって圧縮された１フレームの画像及び音声データである。また、各サブヘッダは、その後に続くデータの長さを示すデータ長情報（Ｌ）を含んでいる。

【００２４】（システムの構成）次に、本実施例によるデジタル・オーディオ・インタラクティブ・システムの概略を、図２に示す。このデジタル・オーディオ・インタラクティブ・システムは、多数のソフトウェアを格納するとともにこのソフトウェアをクライアントからのリクエストに応じて配送するサービスプロバイダと、配送されたソフトウェアを受け取ってこれを再生する多数のサービスクライアントから、構成されている。本実施例によるデジタル・オーディオ・インタラクティブ・システムの構成は、データ識別ＩＤ（ＩＤ）及び時刻情報（ＰＣＲ）を暗号化のために利用して、同一の平文データ（未暗号化のデータのことを言う。以下同じ。）が暗号化されても、常に、異なる内容の暗号文を作り上げる工夫をしたものである。以下、サービスプロバイダ及びサービスクライアント毎に、その詳細な構成を説明する。

【００２５】〔サービスプロバイダ〕サービスプロバイダ内において乱数発生器１は、各ソフトウェアのタイトル毎に、１週間に一度、乱数系列を生成する。この乱数系列は、鍵ブロック単位（予め定められた暗号用鍵の桁）２個分の長さを有し、第１鍵バッファ１６，第２鍵バッファ１７，及び鍵用第１ＤＥＳ（Data Encryption Standard）４に入力される。

【００２６】鍵生成手段としての第１鍵バッファ１６は、この乱数系列から先頭の鍵ブロック単位を切り出して、これを第１タイトル鍵（Ｋｓ１）として、次回の乱数系列の入力があるまでこの第１タイトル鍵（Ｋｓ１）を保持する。

【００２７】同様に、鍵生成手段としての第２鍵バッファ１７は、この乱数系列から２番目の鍵ブロック単位を切り出して、これを第２タイトル鍵（Ｋｓ２）として、次回の乱数系列の入力があるまでこの第２タイトル鍵（Ｋｓ２）を保持する。

【００２８】鍵用第１ＤＥＳ暗号化回路４は、第１タイトル鍵（Ｋｓ１）及び第２タイトル鍵（Ｋｓ２）からなる乱数系列を、第１マスタ鍵（Ｋ１）を用いて暗号化する。暗号化された乱数系列は、鍵用第２ＤＥＳ暗号化回路５に渡され、第２マスタ鍵（Ｋ２）を用いて更に暗号化される。

【００２９】このようにして二重に暗号化された乱数系列は、特定のタイトルに対するタイトル鍵であるとして、鍵ファイル２５内に一旦蓄えられる。この鍵ファイル２５内に蓄えられた暗号化された乱数系列は、１週間後にそのタイトルに対する新たなタイトル鍵用の乱数系列が生成されると、これによって更新される。

10

【００３０】一方、各タイトルのソフトウェアは、乱数発生器１から乱数系列が発生するのに合わせて、週に一回新たなタイトル鍵（Ｋｓ１，Ｋｓ２）によって暗号化されて、蓄積ファイル９に格納される。即ち、蓄積ファイル９に格納されている或るタイトルのソフトウェアは、週に一回更新されるのである。この更新を行うために、平文のデータを格納している同一識別ＩＤ（ＩＤ）を有するトランスポートパケットＰ群は、相対時刻情報（ＰＣＲ）の順に処理を受ける。

【００３１】個々のトランスポートパケットＰのメインヘッダからは、識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）が抽出されて、タイトル用第１ＤＥＳ暗号化回路６及びＤＥＳセット／リセット回路２２に入力される（抽出手段に相当）。それと同時に、メインヘッダからデータ長情報（Ｌ）が抽出されて、データストローブ信号検出器２１に入力される。なお、個々のトランスポートパケットＰのサブヘッダからも、データ長情報（Ｌ）が抽出されて、データストローブ信号検出器（ＳＴ）２１に入力される。このようにして各種情報が抽出されたトランスポートパケットＰは、メインヘッダ側から順に排他ＯＲ回路８の一方の入力端子に入力される。

【００３２】初期化手段としてのＤＥＳセット／リセット回路２２は、入力されたデータから識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）を検知すると、新たなトランスポートパケットＰに対する処理が開始されたと判断して、タイトル用第１ＤＥＳ暗号化回路６及びタイトル用第２ＤＥＳ暗号化回路７をリセットしてそれらの内部状態を初期状態にする。この結果、本実施例では、各トランスポートパケットＰの先頭において暗号同期がとられることになる。即ち、新たなトランスポートパケットＰが入力されて識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）が入力される毎に、両タイトル用ＤＥＳ暗号化回路６，７が初期化されて、この識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）を初期値として暗号化が再開されることになる。

【００３３】第１の暗号化回路としてのタイトル用第１ＤＥＳ暗号化回路６は、第１鍵バッファ１６に保持されている第１タイトル鍵（Ｋｓ１）を用いて、入力情報を暗号化する。タイトル用第１ＤＥＳ暗号化回路６は、リセット後の初期状態においては、識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）を初期値として暗号化するが、以後再度リセットされるまではタイトル用第２ＤＥＳ暗号化回路６から帰還されるデータを暗号化する。

【００３４】第２の暗号化回路としてのタイトル用第２ＤＥＳ暗号化回路７は、第２鍵バッファ１７に保持されている第２タイトル鍵（Ｋｓ２）を用いて、タイトル用第１ＤＥＳ暗号化回路６からの入力情報を更に暗号化する。この結果、撹乱性が更に高められる。タイトル用第２ＤＥＳ暗号化回路７の出力は、タイトル用第１ＤＥＳ暗号化回路６の入力端に帰還されるとともに排他ＯＲ回

路８の他方の入力端子に入力される。この帰還は、ＤＥＳセット／リセット回路２２によって各タイトル用ＤＥＳ暗号化回路６，７がリセットされるまで繰り返される。

【００３５】暗号化制御回路としてのデータストローブ信号検出器（ＳＴ）２１は、トランスポートパケット内のデータのみを暗号化処理するため、各トランスポートパケットＰのメインヘッダからデータ長情報（Ｌ）を抽出し、このデータ長情報（Ｌ）に基づいて各タイトル用ＤＥＳ暗号化回路６，７の暗号化を開始／停止させる制御信号，即ちデータストローブを出力する。即ち、このデータストローブは、各トランスポートパケットＰ内における各データの頭部分が排他ＯＲ回路８に入力されたタイミングで、各タイトル用ＤＥＳ暗号化回路６，７による暗号化を開始させ、各データの末端部分が排他ＯＲ回路８を通過したタイミングで、各タイトル用ＤＥＳ暗号化回路６，７による暗号化を停止させるパルスである。なお、データストローブによって暗号化が停止されていると、タイトル用第２ＤＥＳ暗号化回路７は、“０”を出力し続ける。

【００３６】排他ＯＲ回路８は、平文のトランスポートパケットＰの内容とタイトル用第２ＤＥＳ暗号化回路７からの暗号化データとの排他論理和を出力する。即ち、排他ＯＲ回路８は、各トランスポートパケットＰ内のヘッダ（メインヘッダ及びサブヘッダ）の部分が入力された時には、両タイトル用ＤＥＳ暗号化回路６，７が暗号化を行っていないので、このヘッダの内容を平文のまま出力する。また、各トランスポートパケットＰ内のデータの部分が入力された時には、両タイトル用ＤＥＳ暗号化回路６，７が暗号化を行っているので、タイトル用第２ＤＥＳ暗号化回路７からの暗号化情報に従って入力データの論理値を反転させて出力する。

【００３７】このようにして、平文のヘッダ（メインヘッダ，サブヘッダ）を付した暗号化データが作り出され、蓄積ファイル９に蓄積される。同じ識別ＩＤを有する次の相対時刻情報（ＰＣＲ）を備えたトランスポートパケットＰが処理対象になると、両タイトル用ＤＥＳ暗号化回路６，７がリセットされて、そのトランスポートパケットＰの識別ＩＤ及び相対時刻情報（ＰＣＲ）を初期値として新たな暗号化が行われる。このようにして、或るタイトルを構成する全ての暗号化データが蓄積ファイル９に蓄積されるのである。この時、同じタイトルのソフトウェアについての暗号化データが既に蓄積ファイル９内に蓄積されている時には、新たな暗号化データによって古い暗号化データを更新する。

【００３８】このようにして蓄積ファイル９に蓄積された各タイトルの暗号化データ（トランスポートパケットＰ）は、何れかのサービスクライアントからの要求に応じて、相対時刻情報（ＰＣＲ）の順に蓄積ファイル９から読み出され、データ配送手段としてのトランスポート層伝送路を介して要求元のサービスクライアントに配送される。このとき、配送される暗号化データ（トランスポートパケットＰ）のタイトルに対応する暗号化乱数系列も、鍵ファイル２５から読み出され、トランスポート層のユーザ割当パケットの一部（鍵配送手段としてのセッション層伝送路）を利用してサービスクライアントに配送される。

【００３９】〔サービスクライアント〕サービスクライアント内において、セッション層伝送路を介して受信された暗号化乱数系列は、鍵用第１ＤＥＳ復号化回路１２に入力される。この鍵用第１ＤＥＳ復号化回路１２は、第１マスタ鍵（Ｋ１）１０を利用して、鍵用第１ＤＥＳ暗号化回路４と全く逆のアルゴリズムを実行して復号化を行う。なお、この第１マスタ鍵（Ｋ１）１０は、サービスプロバイダ側のものと全く同じ内容の固定鍵である。

【００４０】鍵用第１ＤＥＳ復号化回路１２の出力は、鍵用第２ＤＥＳ復号化回路１３に入力される。この鍵用第２ＤＥＳ復号化回路１３は、第２マスタ鍵（Ｋ２）１１を利用して、鍵用第２ＤＥＳ暗号化回路５と全く逆のアルゴリズムを実行して復号化を行う。なお、この第２マスタ鍵（Ｋ２）１１は、サービスプロバイダ側のものと全く同じ内容の固定鍵である。

【００４１】これら２段の復号化プロセスを通過した鍵用第２ＤＥＳ復号化回路１３の出力は、乱数発生器１から発生した乱数系列そのものとなる。この乱数系列は、第１鍵バッファ１８及び第２バッファ１９に夫々入力される。

【００４２】第１鍵バッファ１８は、この乱数系列から先頭の鍵ブロック単位を切り出して、これを第１タイトル鍵（Ｋｓ１）として、次回の乱数系列の入力があるまでこの第１タイトル鍵（Ｋｓ１）を保持する。

【００４３】同様に、第２鍵バッファ１９は、この乱数系列から２番目の鍵ブロック単位を切り出して、これを第２タイトル鍵（Ｋｓ２）として、次回の乱数系列の入力があるまでこの第２タイトル鍵（Ｋｓ２）を保持する。

【００４４】一方、トランスポート層を介して受信されたトランスポートパケットＰは、順番に排他ＯＲ回路２０に入力される。この排他ＯＲ回路２０に入力される前に、各トランスポートパケットＰのメインヘッダからは、予め、識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）が抽出されて、タイトル用第１ＤＥＳ復号化回路１４及びＤＥＳセット／リセット回路２４に入力される（第２の抽出手段に相当）。それと同時に、メインヘッダからデータ長情報（Ｌ）が抽出されて、データストローブ信号検出器２３に入力される。なお、個々のトランスポートパケットＰのサブヘッダからも、データ長情報（Ｌ）が抽出されて、データストローブ信号検出器（ＳＴ）２３に入力される。

13

【００４５】ＤＥＳセット／リセット回路２４は、入力されたデータから識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）を検知すると、新たなトランスポートパケットに対する処理が開始されたと判断して、タイトル用第１ＤＥＳ暗号化回路１４及びタイトル用第２ＤＥＳ暗号化回路１５をリセットしてそれらの内部状態を初期状態にする。なお、上述したように、本実施例では、各トランスポートパケットの先頭において暗号同期がとられる。従って、通信路の誤り及び切断があった時には、サービスクライアント内において、次のトランスポートパケットの先頭を検出して両タイトル用ＤＥＳ暗号化回路１４，１５をリセットすれば、自律的に同期状態に復帰することができる。

【００４６】第３の暗号化回路としてのタイトル用第１ＤＥＳ暗号化回路１４は、第１鍵バッファ１８に保持されている第１タイトル鍵（Ｋｓ１）を用いて、入力データを、サービスプロバイダのタイトル用第１ＤＥＳ暗号化回路６と同じアルゴリズムで暗号化する。タイトル用第１ＤＥＳ暗号化回路１４は、リセット後の初期状態においては、識別ＩＤ（ＩＤ）及び相対時刻情報（ＰＣＲ）を初期値として暗号化するが、以後再度リセットされるまではタイトル用第２ＤＥＳ暗号化回路１５から帰還されるデータを暗号化する。

【００４７】第４の暗号化回路としてのタイトル用第２ＤＥＳ暗号化回路１５は、第２鍵バッファ１９に保持されている第２タイトル鍵（Ｋｓ２）を用いて、タイトル用第１ＤＥＳ暗号化回路１４からの入力データを、サービスプロバイダのタイトル用第２ＤＥＳ暗号化回路７と同じアルゴリズムで更に暗号化する。タイトル用第２ＤＥＳ暗号化回路１５の出力は、タイトル用第１ＤＥＳ暗号化回路１４の入力端に帰還されるとともに排他ＯＲ回路２０の他方の入力端子に入力される。この帰還は、ＤＥＳセット／リセット回路２４によって各タイトル用ＤＥＳ暗号化回路１４，１５がリセットされるまで繰り返される。

【００４８】データストローブ信号検出器（ＳＴ）２３は、トランスポートパケットＰ内のデータのみを暗号化処理するため、各トランスポートパケットＰのメインヘッダからデータ長情報（Ｌ）を抽出し、このデータ長情報（Ｌ）に基づいて各タイトル用ＤＥＳ暗号化回路１４，１５の暗号化を開始／停止させる制御信号，即ちデータストローブを出力する。即ち、このデータストローブは、各トランスポートパケットＰ内における暗号化されたデータ部分が排他ＯＲ回路２０に入力されている時のみ、各タイトル用ＤＥＳ暗号化回路１４，１５による暗号化を行わしめるパルスである。なお、データストローブによって暗号化が停止されていると、タイトル用第２ＤＥＳ暗号化回路１５は、“０”を出力し続ける。

【００４９】以上のように、サービスクライアントにおける第１鍵バッファ１８及び第２鍵バッファ１９以降の

14

回路は、サービスプロバイダのものと全く同じである。従って、排他ＯＲ回路２０に入力されるタイトル用第２ＤＥＳ暗号化回路１５からの暗号化情報も、サービスプロバイダにおける排他ＯＲ回路８に入力されるタイトル用第２ＤＥＳ暗号化回路７からの暗号化情報と全く同じである。そのため、排他ＯＲ回路２０は、各トランスポートパケットＰ内のヘッダ（メインヘッダ及びサブヘッダ）の部分が入力された時には、このヘッダの内容を平文のまま出力する。また、各トランスポートパケットＰ内のデータの部分が入力された時には、タイトル用第２ＤＥＳ暗号化回路１５からの暗号化情報に従って論理値を反転させて出力する。この暗号化データは、暗号化によってその論理値が元々反転されていたものである。よって、排他ＯＲ回路２０における再反転によって、その論理値が元の状態に戻るので、暗号化前の平文のデータを復元することができるのである。

《実施例の作用》以上のように、本実施例では、サービスプロバイダ及びサービスクライアント側双方において、タイトル用ＤＥＳ暗号化回路を二重にしている。従って、暗号化アルゴリズムが強化されているので、第三者（ユーザを含む）がトランスポートパケットに基づいて二つのタイトル鍵を解読して、暗号化データを復号化することが、非常に困難となった。このことを図４及び図５を基づいて説明する。

【００５０】いま、かりに、タイトル用第１ＤＥＳ暗号化回路１４に値“Ｉ”を入力したら、タイトル用第２ＤＥＳ暗号化回路１５の出力端に値“Ｏ”が出力されたとする。この場合に第１鍵バッファ１８及び第２鍵バッファ１９に保持されているタイトル鍵Ｋｓ１，Ｋｓ２を解読するには、図４に示すように、タイトル用第１ＤＥＳ暗号化回路１４に既知の値“Ｉ”を入力し続け、本来のタイトル鍵Ｋｓ１に変えて種々の値（推定鍵：Ｋｓ１ｍ）とこれらに対するタイトル用第１ＤＥＳ暗号化回路１４の出力値“Ｃ”を測定する。そして、測定された推定鍵（Ｋｓ１ｍ）と出力値“Ｃ”との関係を、図５に示すように表３０にまとめる。

【００５１】同様に、タイトル用第２ＤＥＳ暗号化回路１５に種々の推定鍵（Ｋｓ２ｍ）を入力して、このタイトル用第２ＤＥＳ暗号化回路１５の出力が既知の値“Ｏ”を維持する入力値“Ｃ”を測定する。そして、測定された推定鍵（Ｋｓ２ｍ）と入力値“Ｃ”との関係を、図５に示すように表３２にまとめる。

【００５２】このようにして作成した二つの表３０，３２を対比した場合に、両表に同じ中間値“Ｃ１ｋ”が表れたら、この値“Ｃ１ｋ”に対応する推定鍵“Ｋｓ１”，“Ｋｓ２”が、夫々第１タイトル鍵Ｋｓ１，第２タイトル鍵Ｋｓ２であると解読できる。

【００５３】このような鍵の解読法（鍵総暗探解読：中間一致攻撃）は、しかしながら、多くの処理時間とメモリ資源を必要とする。例えば、７０ビットの平文，暗号

15

文ペアの場合には、2^{n}回の手続き回数が必要であり、また、上記表を作成するために2^{n}ワード（１ワード６４ビット）のメモリが必要になる。従って、内部１６段のＤＥＳ回路を２段にすると、事実上解読が困難になるのである。

【００５４】なお、比較のために、ＤＥＳ回路を一段にしたときの鍵総暗探解読を説明すると、既知の入力値に対して既知の出力値を出力する推定鍵を探し出すだけで良いので、処理の手間が大幅に経る。上記例に沿うと、７０ビットの平文，暗号文ペアの場合には、2^{n}回の手続き回数のみで成功可能であるので、Ｗｉｅｎｅｒの１０万ドル装置で３５時間程度で解読できてしまう。その結果、本実施例では、タイトル鍵の更新を週１回程度にすることができる。よって、通信路容量をタイトル鍵配送のために消費してしまう問題を解決し、サービスプロバイダーサービスクライアント間の情報転送効率を向上させることができる。

【００５５】なお、このようなタイトル鍵配送回数を激減させるには、暗号同期を鍵更新から切り離して行う必要が、副次的に生じる。本実施例では、暗号同期を、データを配送するためのトランスポートパケットのヘッダに格納されている識別ＩＤ（ＩＤ）と相対時刻情報（ＰＣＲ）によって行っているので、タイトル鍵配送回数を激減させても暗号同期を行うことができる。しかも、この相対時刻情報（ＰＣＲ）がトランスポートパケットの生成時間に依って異なる値をとる。従って、全く同じ内容の平文データが暗号化される場合でも、この平文データを暗号化したデータは全く異なるデータとなる。

【００５６】

【発明の効果】以上のように構成された本発明の暗号化処理方式によると、鍵の頻繁な変更が少なくなり、また、暗号同期信号はシステムに予め備わっている時刻情報を活用することから、暗号アルゴリズムの強化及び暗号同期の為、ユーザパケットの一部を犠牲にする必要がなくなる。

16

【図面の簡単な説明】

【図１】　本発明の原理を示す原理図

【図２】　本発明の一実施例による暗号化処理方式が適用されたデジタル・オーディオ・インタラクティブ・システムの概略図

【図３】　一つのソフトウェアを構成するデータが格納された各トランスポートパケットの構造を示す説明図

【図４】　中間一致攻撃による鍵総暗探解読方式の説明図

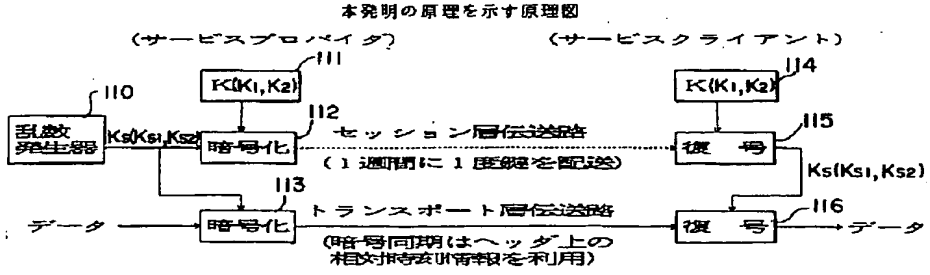
【図５】　中間一致攻撃による鍵総暗探解読方式の説明図

【図６】　従来の暗号化処理方式の概略説明図

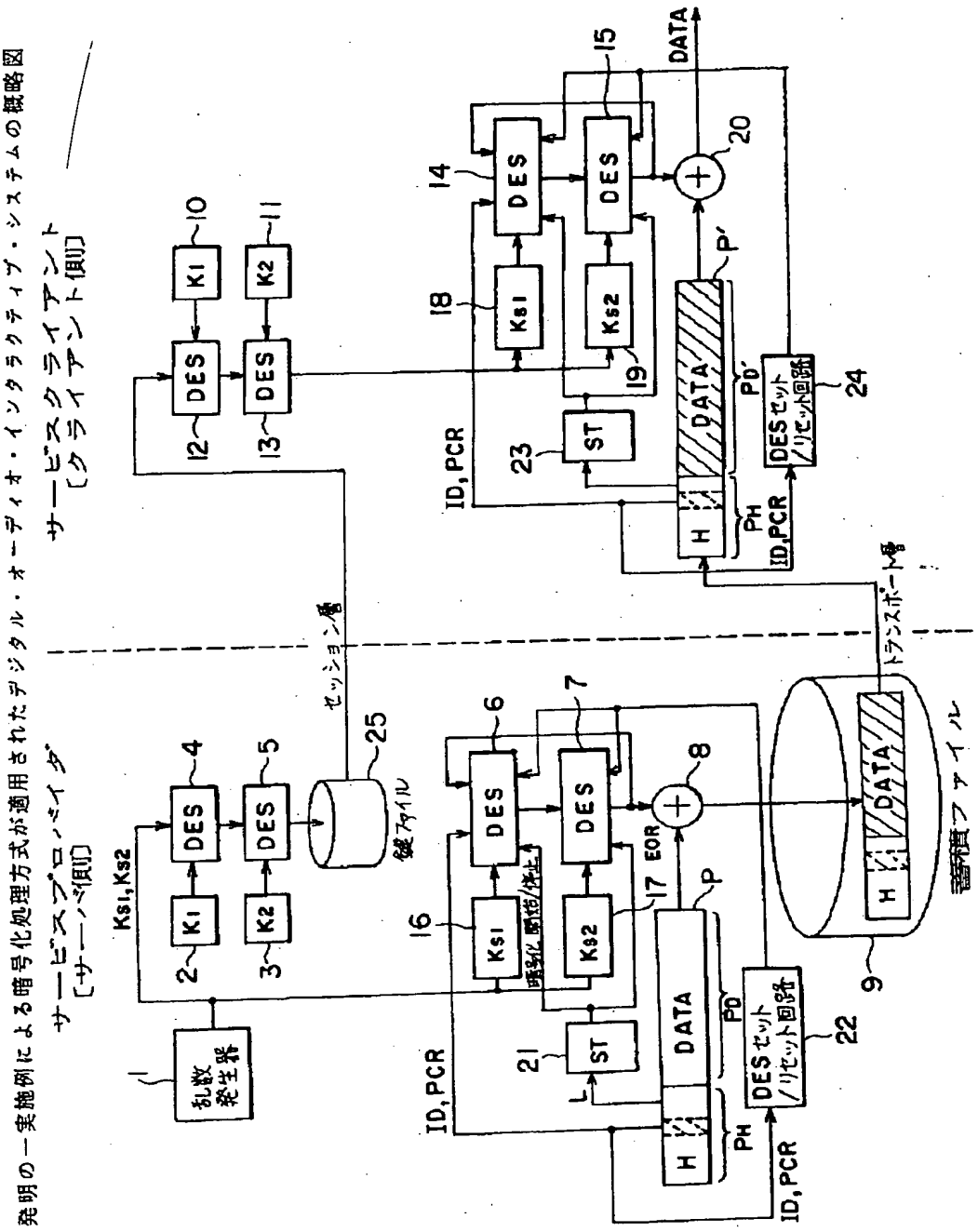
【符号の説明】

１　乱数発生器
６　タイトル用第１ＤＥＳ暗号化回路
７　タイトル用第２ＤＥＳ暗号化回路
８　排他ＯＲ回路
１４　タイトル用第１ＤＥＳ暗号化回路
１５　タイトル用第２ＤＥＳ暗号化回路
１６　第１タイトル鍵バッファ
１７　第２タイトル鍵バッファ
１８　第１タイトル鍵バッファ
１９　第２タイトル鍵バッファ
２０　排他ＯＲ回路
２１　データストローブ信号検出器（ＳＴ）
２２　ＤＥＳセット／リセット回路
２３　データストローブ信号検出器（ＳＴ）
２４　ＤＥＳセット／リセット回路

【図１】

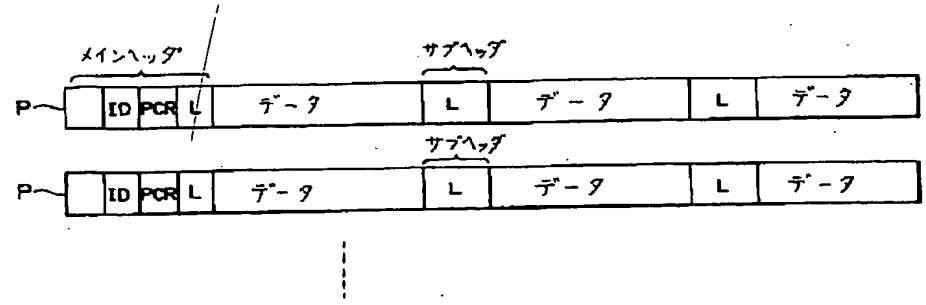


【図２】


本発明の一実施例による暗号化処理方式が適用されたデジタル・オーディオ・インタラクティブ・システムの概略図
サービスプロバイダ
〔サーバ側〕
サービスクライアント
〔クライアント側〕
乱数発生器
DES
K1
K2
Ks1, Ks2
鍵ファイル
セッション層
トランスポート層
ST
DATA
H
PH
PD
ID, PCR
EOR
DESセット/リセット回路
暗号化/復号/停止
蓄積ファイル

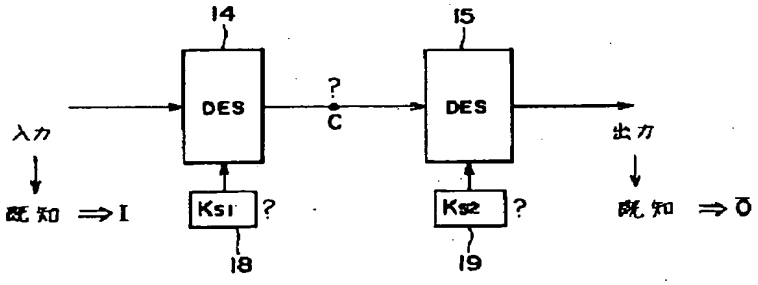
【図３】

一つのソフトウェアを構成するデータが格納された各トランスポートパケットの構造を示す説明図



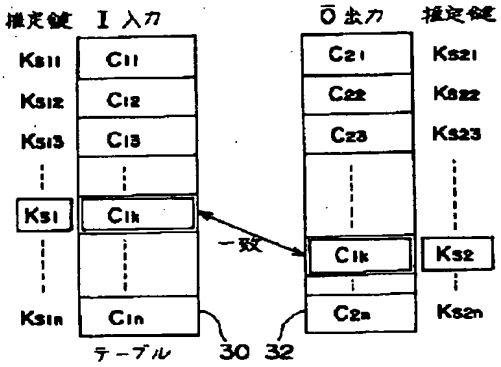
【図４】

中間一致攻撃による鍵総当たり解読方式の説明図



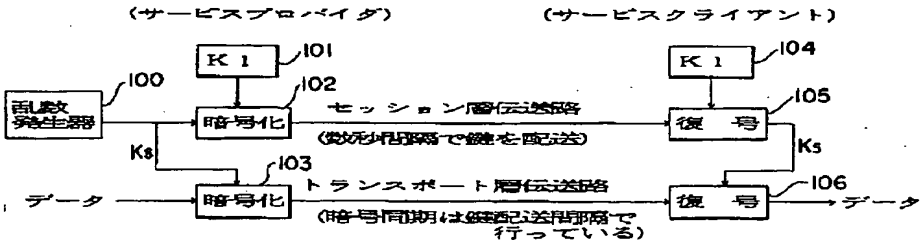
【図５】

中間一致攻撃による鍵総当たり解読方式の説明図



【図６】

従来の暗号化処理方式の概略説明図



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
9/12				
H04N 7/167				

(72)発明者　古賀　醸
神奈川県川崎市中原区上小田中１０１５番
地　富士通株式会社内
(72)発明者　石崎　正之
神奈川県川崎市中原区上小田中１０１５番
地　富士通株式会社内
(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中１０１５番
地　富士通株式会社内